

\$5M NSF award to enhance data protections for users nationwide

ASU and collaborators to develop privacy-enhancing cybersecurity infrastructure

By Sandy Keaton Leander, ASU News
September 18, 2026

Imagine the following scenarios: Medical researchers at two different institutions need to compare patient data to advance drug discovery. Cybersecurity professionals want to discuss intelligence related to attacks in their networks to defend against adversaries.

However, privacy concerns and safeguards, as well as legal regulations, can prevent them from sharing and collaborating on sensitive information, including personally identifiable information or intellectual property.

With \$5 million from the U.S. National Science Foundation Office of Advanced Cyberinfrastructure, researchers from Arizona State University, in partnership with San Diego State University and University of Utah, will develop a national community resource for computing and sharing private data.

Over the next five years, the team will deploy and support a novel cyberinfrastructure called Prototype Architecture for Research Advances using Privacy Enhancing Technologies that could be used in a range of fields that require data analysis, including health care, internet security, science, finance and the social sciences, to protect sensitive information such as medical records, financial information and census statistics.

Using privacy-enhancing technologies, PARAPET is designed to be a more secure way to share and collaborate on sensitive data, safeguard data at rest and during computation, and train AI models without exposing private data.

[Carolyn Ellis](#), director of the [ASU Research Technology Office](#) and an expert on regulatory and policy compliance, will ensure PARAPET meets the rapidly evolving requirements for technologies like this, and will lead efforts to recruit users from across the nation to test it once a prototype is

ready.

“Privacy-enhancing technologies have enormous potential to change how we conduct research with sensitive or regulated datasets,” said Ellis, a co-principal investigator on the project. “We first need to understand how these new capabilities fit within institutional policies, research workflows, and the privacy expectations established through data-sharing agreements. The ASU team is well positioned to investigate these new research data use cases.”

Through ASU’s leadership of the national [Regulated Research Community of Practice](#), the ASU team will bring a vital institutional perspective to the PARAPET project. This role bridges the gap between new tech capabilities and the practical realities of protecting sensitive research data.

“There are a lot of examples where privacy aspects preclude researchers from working on data together, and that’s an impediment to science,” said Robert Beverly, director of SDSU’s [Cybersecurity Center for Research and Education](#) and professor of computer science.

“Researchers are entrusted with sensitive data, so we need to protect it. Trying to get these technologies into production promises to move the whole field forward.”

How to secure sharable data

Today, data can be encrypted for transmission and storage, but performing computations on encrypted data remains challenging. This project aims to make that process easier.

To secure shared information, researchers plan to equip PARAPET with specialized software and hardware tools that allow one user to send encrypted data that another user can work on without decrypting it, ensuring the data is never revealed to anyone but the original user. In addition, these techniques could help protect against future quantum computing attacks, which pose a heightened threat to cyber systems. PARAPET will provide an important national-scale test bed for the research community to explore these tools and techniques.

PARAPET also seeks to preventatively protect data, so that it remains inaccessible in the event that a device is compromised. In fact, the entire system will be secured by locking away encrypted data so only approved users on secured networks can access it.

Finally, with AI spreading into virtually every discipline, it is essential to protect data as models are built. In response, PARAPET aims to protect users’ data while fine-tuning central AI models that can be used nationwide.

One way to do this is users can train their local model on their own device and share only the model updates with PARAPET, so it can use the information from the updates to train its larger model without accessing the raw data.

Unlike systems that require organizations to transfer raw data to a central service, PARAPET will test methods that allow participating institutions to retain greater control over sensitive research data.

Beverly points out that even anonymizing data is not secure, as many hackers can conduct re-identification attacks by reverse engineering data to link it back to a person. With secure computing

hardware utilizing technologies such as differential privacy, homomorphic encryption and federated learning, PARAPET seeks to provide a vastly more secure option for supporting high performance computing needs.

Manish Parashar, chief AI officer for the University of Utah and executive director of its Scientific Computing and Imaging Institute, will help manage PARAPET's hardware and ensure the infrastructure is ready for deployment at a national scale.

"Data-driven and AI-enabled research is revolutionizing science, but progress in critical fields such as cybersecurity and public health is hampered by our inability to obtain, create, compute on and share regulated data," Parashar said. "PARAPET takes an important step toward solving this problem by leveraging advances in privacy-enhancing technologies. The University of Utah looks forward to contributing expertise and leadership in designing and operating the compliant, regulated environments that PARAPET needs to safely accelerate research with sensitive data."

Bryana Quintana from SDSU and Kelly Hermans from UofU contributed to this article.

This project is made possible through [U.S. National Science Foundation Office of Advanced Cyberinfrastructure grant #2537035](#).

This story originally appeared on [ASU News](#).

Main image

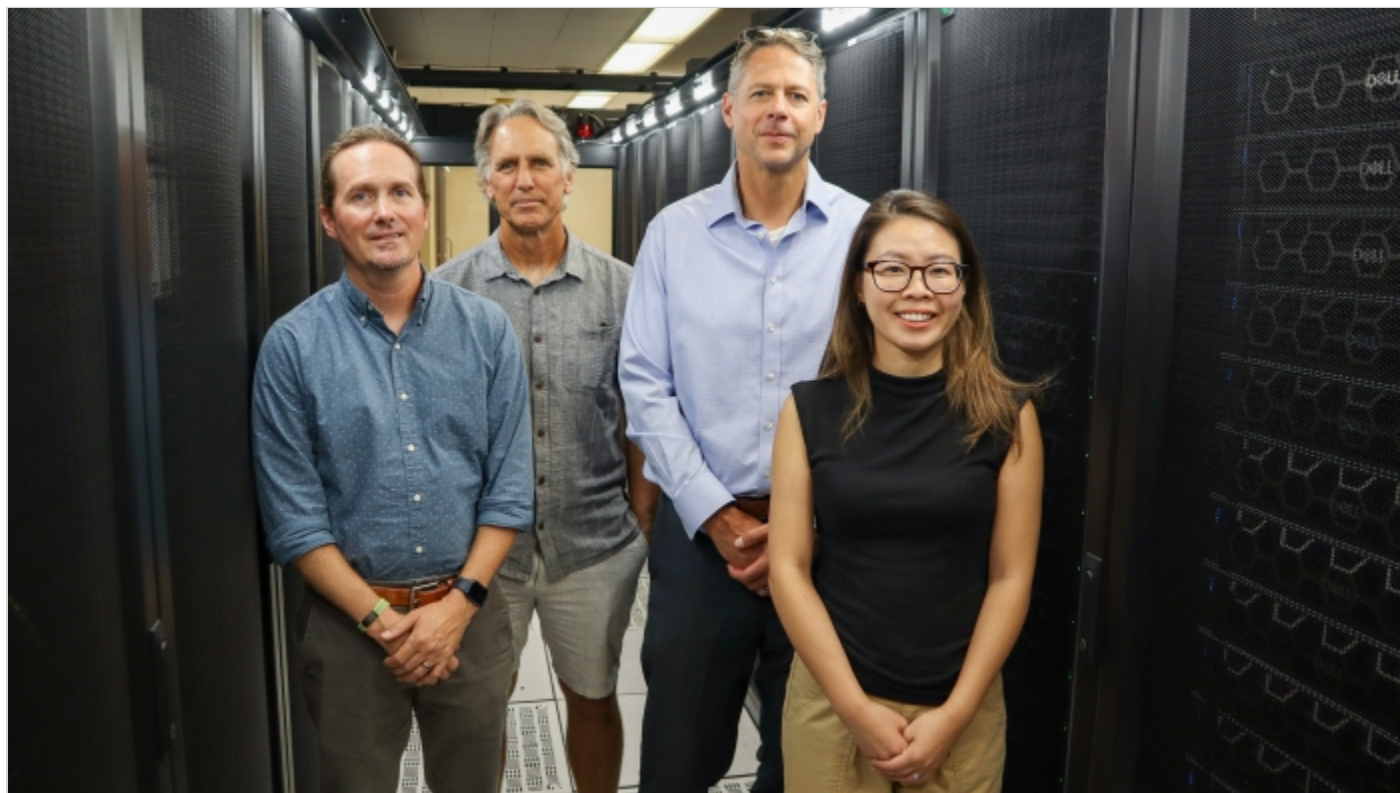


Researchers from ASU and two university partners are developing a novel cyber-infrastructure with the goal of protecting privacy and sensitive data while improving computing collaboration between institutions. Illustration by Andy Keena/ASU

Text image(s)



Carolyn Ellis



From left: SDSU's Mike Farley, Shawn Strande, Robert Beverly and Joann Chen. Photo courtesy of Bryana Quintana



Manish Parashar